METHOD AND APPARATUS FOR PROVIDING A KEY DISTRIBUTION CENTER WITHOUT STORING LONG-TERM SERVER SECRETS

ABSTRACT

One embodiment of the present invention provides a system for operating a key distribution center (KDC) that provides keys to facilitate secure communications between clients and servers across a computer network, wherein the system operates without having to store long-term server secrets. The system operates by receiving a communication from a server at the KDC. This communication includes an identifier for the server, as well as a temporary secret key to be used in communications between a client and the server for a limited time period. In response the communication, the system attempts to authenticate the server. If the server is successfully authenticated, the system stores the temporary secret key at the KDC, so that the temporary secret key can be subsequently used to facilitate communications with the server. Upon subsequently receiving a request at the KDC from a client that desires to communicate with the server, the system produces a session key to be used in communications between the client and server, and then creates a ticket to the server by encrypting an identifier for the client and the session key with the temporary secret key for the server. Next, the system assembles a message that includes the identifier for the server, the session key and the ticket to the server, and sends the message to the client in a secure manner. The system subsequently allows the client to forward the ticket to the server in order to initiate communications between the client and the server.